

FILED

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

2016 SEP 20 PM 4:47

CLERK US DISTRICT COURT
WESTERN DISTRICT OF TEXAS

BY KICK DEPUTY

UNITED STATES OF AMERICA,

Plaintiff,

v.

CHIMENE HAMILTON ONYERI,
a/k/a, "Chimu,"
a/k/a, "Chimno,"
MARCELLUS ANTOINE BURGIN,
a/k/a, "Southwest,"
a/k/a, "Chi,"
a/k/a, "Chi-town," and
RASUL KAREEM SCOTT,
a/k/a, "N.O.,"

Defendants.

CRIMINAL NO.

INDICTMENT

A16 CR 241 LY

[Violations: Count 1: Conspiracy to Conduct or Participate in an Enterprise Engaged in a Pattern of Racketeering Activity, in Violation of Title 18, United States Code, § 1962(d) [All Defendants]; Count 2: Conspiracy to Commit Mail Fraud, in Violation of Title 18, United States Code, §§ 1349 and 1341 [Defendant Onyeri]; Count 3: Aggravated Identity Theft, in Violation of Title 18 United States Code § 1028A(a)(1) [Defendant Onyeri]; Count 4: Conspiracy to Commit Wire Fraud, in Violation of Title 18 United States Code §§ 1349 and 1343 [Defendant Onyeri]; Counts 5 - 9: Aggravated Identity Theft, in Violation of Title 18 United States Code § 1028A(a)(1) [Defendant Onyeri]; Count 10: Conspiracy to Commit Wire Fraud, in Violation of Title 18 United States Code §§ 1349 and 1343 [All Defendants]; Count 11: Aggravated Identity Theft, in Violation of Title 18 United States Code § 1028A(a)(1) [All Defendants].

THE GRAND JURY CHARGES:

COUNT ONE
Conspiracy to Conduct or Participate in an Enterprise
Engaged in a Pattern of Racketeering Activity
[18 U.S.C. 1962(d)]

The Enterprise

1. At times material to this indictment CHIMENE HAMILTON ONYERI (“ONYERI”) was the leader of a criminal organization that engaged in various types of illegal activity including wire and mail fraud and conspiracy to commit those offenses, identity theft, bribery, money laundering and conspiracy to commit that offense and attempted murder. The Onyeri Criminal Organization, including its leaders, members and associates, constituted an enterprise (hereinafter “the enterprise”) as defined by Title 18, United States Code, § 1961(4), to wit: a group of individuals associated in fact, which enterprise was engaged in and the activities of which affected interstate and foreign commerce. The enterprise constituted an ongoing organization whose members functioned as a continuing unit for a common purpose of achieving the objectives of the enterprise.
2. CHIMENE HAMILTON ONYERI (“ONYERI”) was the leader of the enterprise, directed the activities of the enterprise, recruited members of the enterprise, paid members of the enterprise, protected the existence of the enterprise and devised fraud schemes by which the enterprise would profit. MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT were members of the enterprise and assisted ONYERI in conducting the activities of the enterprise by participating in activities such as converting stolen debit card numbers into cash proceeds and by acting as lookouts and/or drivers for ONYERI during the criminal

operations of the enterprise.

Purposes of the Enterprise

3. The Onyeri Organization's primary purpose was to make money, that is, to enrich ONYERI and the enterprise's associates and members through the commission of a broad range of criminal activities described herein. ONYERI and the other members and associates of the enterprise also engaged in conduct for the purpose of perpetuating the criminal enterprise, protecting its ongoing criminal operations from perceived threats, and shielding it and its criminal affairs from law enforcement authorities.

The Racketeering Conspiracy

4. Beginning on a date unknown, but not later than January 2012, and continuing through and about November 2015, in the Western District of Texas, the Southern District of Texas and the Western District of Louisiana, and elsewhere,

CHIMENE HAMILTON ONYERI,
a/k/a, "Chimu,"
a/k/a, "Chimno,"
MARCELLUS ANTOINE BURGIN,
a/k/a, "Southwest,"
a/k/a, "Chi,"
a/k/a, "Chi-town," and
RASUL KAREEM SCOTT,
a/k/a, "N.O.,"

the defendants herein, being persons employed by and associated with the enterprise, which engaged in, and the activities of which affected, interstate and foreign commerce, knowingly and intentionally combined, conspired and agreed with one another and others known and

unknown, to violate the provisions of Title 18, United States Code, Section 1962(c), that is, to conduct and participate, directly and indirectly, in the conduct of the affairs of the enterprise through a pattern of racketeering activity consisting of multiple acts:

indictable under:

- (a) Title 18, United States Code, §1341 - Mail Fraud;
- (b) Title 18, United States Code, § 201 - Bribery of a Public Official;
- (c) Title 18, United States Code, §1343 - Wire Fraud;
- (d) Title 18, United States Code, § 1028 - Fraud in Connection with Identification Documents, Authentication Features and Information;
- (e) Title 18, United States Code, § 1029 - Access Device Fraud;
- (f) Title 18, United States Code, § 1956(h) - Conspiracy to Commit Money Laundering;
- (g) Title 18, United States Code, § 1956 - Money Laundering; and

involving murder, in violation of Texas Penal Code Sections 15.01, 19.02 and 19.03.

It was part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the enterprise.

Manner and Means

5. ONYERI and other members of the enterprise sought out and learned from others how to commit credit and debit card related fraud using various means and methods, including skimming devices. ONYERI recruited other individuals such as a tax preparer, a mail carrier and a bank employee, who could provide services that allowed the enterprise to utilize

their respective positions to further the enterprise's criminal purposes.

6. ONYERI and other members of the enterprise recruited "workers" to skim credit and debit card numbers from unsuspecting customers at stores or restaurants using skimming devices provided by ONYERI. ONYERI and other members of the enterprise recruited and paid members and associates of the enterprise to enter locations such as Walmart, often wearing disguises provided by ONYERI, to purchase property or gift cards with stolen credit or debit cards.
7. ONYERI and other members of the enterprise constructed or assembled skimming devices and personal identification number ("PIN") readers that could be placed on Automatic Teller Machines ("ATMs") in order to collect unsuspecting victims' debit card and PIN numbers. ONYERI and other members of the enterprise utilized electronic devices to encode stolen debit and credit card numbers onto gift cards or other cards.
8. ONYERI and other members and associates of the enterprise placed skimming devices on ATMs, often wearing disguises and concealing or changing the license plates on the vehicles used to transport members of the enterprise to banks. Once credit card or debit card numbers were illegally skimmed, ONYERI and other members of the enterprise transferred the stolen numbers onto other cards, such as stolen or purchased gift cards, and sometimes used a machine to emboss numbers on the front of those cards so as to make them appear legitimate and to match the stolen credit or debit card numbers that had been encoded onto the back of the cards.
9. ONYERI, MARCELLUS ANTOINE BURGIN, RASUL KAREEM SCOTT and other members and associates of the enterprise used cards manufactured in these ways to withdraw

currency from ATMs or to purchase gift cards loaded with funds or to purchase property which would later be returned for cash, or to send money orders to themselves or others or to purchase chips or credit at a casino. ONYERI, MARCELLUS ANTOINE BURGIN, RASUL KAREEM SCOTT, and other members of the enterprise laundered the illegally acquired funds through one or more of the methods and means described above, among others. ONYERI used the illegal proceeds of these schemes to pay members of the enterprise and to enhance his position as leader of the enterprise, among other things.

10. ONYERI and other members of the enterprise acquired personal identifying information (PII), including social security numbers and names from, among other sources, hospital records so that this stolen PII could be used to fraudulently file tax returns in the victims' names.
11. ONYERI and other members of the enterprise located mailboxes that could be used to receive fraudulently obtained United States Treasury tax refund checks, among other things, to include stored value cards onto which fraudulently obtained tax refunds could be electronically transferred. ONYERI recruited at least one person he believed was a U.S. Postal letter carrier to intercept fraudulently obtained United States Treasury tax refund checks from addresses on the mail carrier's route.
12. ONYERI and other members and associates of the enterprise used the United States mail to file false tax returns in the names of individuals who had their identities stolen.
13. ONYERI and other members and associates of the enterprise utilized a bank employee to facilitate the opening of bank accounts in the names associated with the fraudulently obtained tax refund checks. The opening of these accounts allowed ONYERI and other members and

associates of the enterprise to cash a portion of the United States Treasury refund check and to receive an ATM card which permitted ONYERI and other members and associates of the enterprise to withdraw the rest of the funds from the account.

14. ONYERI and other members and associates of the enterprise used false identification documents to carry out the criminal activities of the enterprise, to include driver's licenses and social security cards.
15. When the existence of the enterprise was threatened, ONYERI, MARCELLUS ANTOINE BURGIN, and RASUL KAREEM SCOTT responded with violence. ONYERI, MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT travelled to Austin, Texas, in order to kill Judge Julie Kocurek, a Texas District Court Judge whom ONYERI believed was going to sentence ONYERI to prison.
16. ONYERI, MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT used a gift card purchased with a skimmed, stolen debit card number to pay for expenses related to the attempted murder of Judge Kocurek. ONYERI, MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT attempted to kill Judge Kocurek outside her home in Austin, Texas by shooting Judge Kocurek while she sat inside of her car on the evening of November 6, 2015.

Special Sentencing Allegation

17. On or about November 6, 2015, in the Western District of Texas, CHIMENE HAMILTON ONYERI, MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT did, with specific intent to commit the offense of the Capital Murder of Julie Kocurek, attempt to

intentionally and knowingly cause the death of Julie Kocurek in retaliation for and on account of the service and status of Julie Kocurek as a Judge of the District Court, by shooting Julie Kocurek with a firearm, which amounted to more than mere preparation that tended but failed to effect the commission of the offense intended, in violation of Texas Penal Code Sections 15.01, 19.02 and 19.03.

All in violation of Title 18, United States Code, § 1962(d).

COUNT TWO
Conspiracy to Commit Mail Fraud
[18 U.S.C. § 1349]

Background

18. “Stolen Identity Refund Fraud” or “SIRF” is a category of schemes that victimize both the United States Treasury and individual taxpayers. Under such schemes, perpetrators file false income tax returns using the identities of actual taxpayers, including the taxpayers’ true personal identifiers such as names, Social Security numbers, addresses, and employers. The identities are stolen, and the taxpayers are unaware of the returns. The returns claim refunds, and the perpetrators arrange for the IRS to pay the fraudulent refunds to them, rather than to the owners of the stolen identities. Perpetrators of such schemes often file the false returns and receive the fraudulent refunds through the United States Mail, or electronically through a bank account or onto a stored value card.

The Scheme

19. ONYERI and co-conspirators, known and unknown to the Grand Jury, acquired the names, Social Security numbers and other personally identifiable information (PII) of victims.

These names were acquired by, among other methods, paying individuals who had access to unsuspecting victims' PII in exchange for the theft of the PII data. ONYERI and other co-conspirators also acquired addresses to which U.S. Treasury refund checks could be sent. These addresses were acquired by, among other methods, locating mailboxes which could be accessed by ONYERI and his co-conspirators, and bribing mail carriers to provide addresses that could be used and to intercept corresponding tax refund checks. Once ONYERI and his co-conspirators acquired the PII and addresses, this information was provided to Co-conspirator #2, who prepared fraudulent tax returns with the stolen PII and addresses. The returns were filled out in the name of the victims whose PII was stolen with one or more of the addresses acquired by ONYERI and his co-conspirators. Tax returns prepared in this way were mailed to the Internal Revenue Service Center in Austin, Texas and refund checks were issued and mailed out by the IRS. Tax refund checks were used to open bank accounts in the names of the victims at one or more banks in Bryan, Texas with the assistance of a bank employee, Co-conspirator #3. Often, a substantial portion of the resultant funds were withdrawn at the bank and the rest of the funds withdrawn at Automatic Teller Machines (ATMs) when they became available.

Manner and Means

The scheme consisted of, and was carried out using, the following means and overt acts, among others:

20. On or about May 16, 2013, ONYERI approached a U.S. Postal Letter Carrier and offered the Letter Carrier money to provide Houston, Texas addresses to ONYERI. ONYERI provided

a telephone number to the Letter Carrier.

21. On or about May 24, 2013, ONYERI, using the number that he provided to the Letter Carrier, spoke to an individual posing as a Letter Carrier, but who was in fact a United States Postal Inspection Service employee, acting in an undercover capacity (UCA). ONYERI told the UCA that ONYERI wanted to meet with the UCA and wanted the UCA to use his position as a Mail Carrier to deliver mail directly to ONYERI. ONYERI told the UCA that ONYERI would have mail sent to addresses and that ONYERI wanted the UCA to intercept the mailings. ONYERI stated in sum and substance:

ONYERI: It's -- you know, like, say, for instance, I do a -- a Turbo Tax in his name - -
 UCA: Okay
 ONYERI: -- or -- Taxslayer; and it's, like --
 UCA: Okay.
 ONYERI: --the information, like, I send out like 2,000 in his name. You see what I'm saying?
 UCA: Okay.
 ONYERI: But I send it to another address. You know what I mean?
 UCA: Okay.
 ONYERI: So his money will come back; but we'll have that 2,000 - - you see what I'm saying?
 ONYERI: I'm just sending them to a different address.
 UCA: Oh, okay. All right. So what you need from me? I mean, like, add—
 ONYERI: I need addresses. Then when the mail come, you call me—
 UCA: Okay.
 ONYERI: --and I pick up and I'll pay you -- I'll pay you around \$1,500.

22. On or about May 31, 2013, ONYERI met with the UCA and informed the UCA that ONYERI knew that tax refund checks were going to be delivered to addresses provided by the UCA.

ONYERI stated, in sum and substance:

ONYERI: Just a regular envelope. It's going to be white -- or it's, like, a white envelope, with -- issue a refund.

During this same conversation, ONYERI called Co-conspirator #2 and asked whether post

office boxes would work for the scheme and told Co-conspirator #2 that he was talking with the mailman right now. During the same meeting, ONYERI also spoke with the UCA about “cashing out” the tax refund checks in College Station, Texas, and told the UCA that ONYERI had a “chick that clean them off for us ... she’s a manager.”

23. On or about May 31, 2013, the UCA provided several apartment addresses to ONYERI. The UCA also provided Houston area apartment addresses to ONYERI on January 15, 2014 and March 22, 2014.
24. On or about September 9, 2013, the UCA recovered a U.S. Treasury tax refund check from one of the addresses previously provided to ONYERI. The UCA then contacted ONYERI to inform ONYERI that a check had been intercepted and ONYERI told the UCA to open the envelope and tell ONYERI the amount. When the UCA told ONYERI that the check was for \$5,800.00, ONYERI stated, in sum and substance, “That’s my number.”
25. On September 10, 2013, ONYERI met with the UCA for the purposes of receiving the \$5,800.00 U.S. Treasury tax refund check. During this meeting, ONYERI discussed Co-conspirator #3, who worked at the bank in College Station, Texas and Co-conspirator #3’s ability to open bank accounts. ONYERI stated in sum and substance, and among other things, “So, after I finish wiring off, I’m going to take that right there to – to fucking College Station. I let the check in College Station... I’m calling – and then my little chick down at the bank, man, a bitch done got her fired, dog. She putting in her two weeks’ notice. Like, we brung, like over fifty thousand to her, like... She is a manager.” ONYERI further stated, in sum and substance, “... so she’d take them and she’d drop them off in the account and she’d cash them for me. She’s a manager. She’d open the account, and she’d cash them. So we dropped

off..." When asked by the UCA if she opened the account in "home boy's" name, ONYERI stated in sum and substance, "In home boy name, that's why I was asking you for the name." ONYERI had in fact previously asked the UCA for the name on the \$5,800.00 check.

26. On or about September 10, 2013, Co-Conspirator #3 opened an account in the name of the individual to whom the \$5,800.00 refund check was issued.
27. On May 28, 2013, ONYERI and Co-Conspirator #1 were stopped in a vehicle in Houston, Texas. At that time, ONYERI and Co-conspirator #1 possessed five U.S. Treasury checks in various victims' names. None of these five victims filed the tax return that resulted in the refund checks recovered on May 28, 2013. The refund checks totaled \$8,892.00.
28. On or about March 10, 2014, ONYERI spoke with the UCA and explained that ONYERI had paid for a system that allowed ONYERI and his co-conspirators to issue refund checks directly but that even though ONYERI no longer needed the services of the UCA, he would still pay the UCA.
29. On or about March 26, 2014, ONYERI again described the new system that he and his co-conspirators were using, and mentioned another mailman that ONYERI was paying. In sum and substance, ONYERI stated:

ONYERI: Another thing is I got someone doin' - - doin' it the other way, too, that I paid for. So that's what I'm talkin' about. But, you know - - you know, I'm an exceptional - -exceptional employer, dog. I don't get - - let me - - I'm thrilled, bro. I don't give a damn if you - - if you have nothin' to do with it. I make sure everybody eat from the same table, homey.

UCA: Right.

ONYERI: So even though I paid for that system - - even though I paid for that system and that don't have nothin' to do with you guys, I'll still pay y'all. Y'all still get a cut out of that. That's just how I (unintelligible).

ONYERI: It's five of them that I cleared. I was with my sista last night. You know, I mean, because, you know, they shut down the system on this over - - she lost a bunch of checks. She lost - - you know what I mean? The - - blank

checks to where we print them out on because, you know, the government - - we insured by the government, dog, so she lost them. She - - so we had to go file a police report and all that shit and they put everything on - - a freeze. So they just released it back for us so my sista can get to doin' what she do. So - -

UCA: You mean the police - - the police didn't ask no questions? What - - what police department is that? Shit.

ONYERI: Yeah. Now, they - - you know - - you know, I'm - - I'm smart. Hey - - hey, booboo, I'm smarter than the average bear. You know what I'm sayin'?

UCA: That must have been that wacky ass Harris County, man.

ONYERI: Yeah. I'll be able to be more in depth with you when I see you, man, but I'm just - - right when they cash out, homey, (unintelligible) everything. I mean, right when they - - when we get the checks come in, it should be in - - she say anytime from now this week before the week I'm gonna go cash out and you meet up with men. You pay yourself and I've gotta pay my other mailman, too.

The Charge

30. Paragraphs 19 through 29 of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.
31. Beginning on a date unknown, but no later than in or about March 2012, and continuing to at least in and about June 2014, in the Western District of Texas and elsewhere, the Defendant,

CHIMENE HAMILTON ONYERI, a/k/a, "Chimu," a/k/a, "Chimno,"

Did knowingly and willfully conspire and agree with co-conspirators, known and unknown to the Grand Jury, to commit offenses against the United States, namely Mail Fraud, in violation of Title 18, United States Code, Section 1341, that is, having devised and having intended to devise a scheme and artifice, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, knowingly and with

intent to defraud or the purpose of executing the scheme, caused to be mailed by means of the United States Postal Service a U.S. Individual Income Tax Return, "Form 1040A," which income tax returns included the names and Social Security numbers of victims who had their personally identifiable information stolen, and fraudulently requested refunds in those individuals' names, and that said Forms 1040A were mailed to the Internal Revenue Service Center in Austin, Texas.

All in violation of Title 18, United States Code, Sections 1349 and 1341.

COUNT THREE
Aggravated Identity Theft
[18 U.S.C. § 1028A]

32. On or about July 17, 2013, in the Western District of Texas, and elsewhere, the Defendant,

CHIMENE HAMILTON ONYERI, a/k/a, "Chimu," a/k/a, "Chimno,"

did knowingly transfer, possess and use, without lawful authority, a means of identification of another person, to wit, a name and Social Security number of Victim #1, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c)(5), namely Conspiracy to Commit Mail Fraud, as charged in Count Two of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNT FOUR
Conspiracy to Commit Wire Fraud
[18 U.S.C. § 1349]

Background

33. “Credit or Debit Card Skimming” is a fraudulent scheme in which perpetrators utilize mechanical devices to capture credit card or debit card numbers from unsuspecting victims. This can be accomplished using a magnetic card reader that stores credit and debit card numbers. The stolen credit or debit card numbers are then used by perpetrators to obtain cash or goods. The scheme often involves an intermediate step or steps before the stolen card numbers are converted into cash proceeds. If goods are purchased, these goods are often sold for cash. Gift cards are also used. The gift cards are “loaded” with funds from the victims’ accounts and then used to purchase goods, which are sold for cash or returned to store for cash refunds. Perpetrators use this kind of “layering” to avoid detection by law enforcement.

The Scheme

34. ONYERI and others, known and unknown to the Grand Jury, participated in a credit card skimming scheme from at least in or about December 2011 to in or about November 2013. “Skimming” is the process by which victims’ credit card numbers are captured on a device, or “skimmer,” so that they can be used to illicitly purchase items and obtain funds. ONYERI and Co-conspirator #1 recruited “workers” to skim debit and credit cards from retail locations in the Houston, Texas area. ONYERI supplied a skimming device and paid the workers to illicitly collect debit and credit card numbers from unsuspecting customers of these retail locations. ONYERI and Co-conspirator #1 would meet with the workers and

upload the stolen credit and debit card numbers. The stolen debit and credit card numbers were then loaded onto gift cards. On some occasions, Co-conspirator #1 washed the raised or embossed numbers off of the gift cards and ONYERI would encode the stolen card numbers onto gift cards which would then be embossed with a number to make them look authentic. ONYERI and Co-conspirator #1 would then use the gift cards to purchase iPads which were then sold for approximately \$400 to \$600. The stolen debit card numbers were also used to purchase Money Gram money orders which would be converted to cash. Co-conspirator #1 and other co-conspirators, known and unknown to the Grand Jury, worked at ONYERI's direction in the scheme and received a portion of the criminal proceeds.

Manner and Means

The scheme consisted of, and was carried out using, the following means and overt acts, among others:

35. On or about March 25, 2012, ONYERI and Co-conspirator#1 traveled into the Western District of Texas for the purposes of committing the credit card scheme. ONYERI and Co-conspirator #1 were stopped by the Rollingwood Police Department for speeding on Bee Caves Road, in Rollingwood, Texas. The vehicle in which they were traveling had a fictitious temporary, paper license tag, which had been placed on the rear of the vehicle in order to conceal the identity of vehicle and its occupants as they perpetrated the fraud scheme. Inside the vehicle ONYERI and Co-conspirator #1 possessed, among other items, a credit card reader and in excess of seventy (70) gift cards. These items, among others, were possessed in order to perpetrate the fraudulent scheme described herein.

36. The numbers/accounts that were encoded onto the magnetic strips of some of the gift cards did not match the numbers embossed on the front of the gift cards. Several of the gift cards had been encoded with numbers that were compromised, that is, skimmed or stolen. At least one of the compromised (stolen) American Express Card numbers (card number ending 27000) was used to make purchases of American Express gift cards at a Randall's Supermarket and at an Office Depot, both located in Austin, Texas, within the Western District of Texas.
37. These transactions were processed through a third party processor, located in Phoenix, Arizona, and payments were then made to the merchant from a Wells Fargo Bank located in Tampa, Florida. Thus, ONYERI caused to be transmitted by means of wire communication in interstate commerce the signals and sounds described herein when conducting the fraudulent transactions within the Western District of Texas.

The Charge

38. Paragraphs 34 through 37 of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.
39. From at least in or about December 2011 to in or about November 2013, the exact dates being unknown, in the Western District of Texas and elsewhere, the Defendant,

CHIMENE HAMILTON ONYERI, a/k/a, "Chimu," a/k/a, "Chimno,"

did knowingly and willfully conspire and agree with others known and unknown to the Grand Jury, to commit certain offenses against the United States, namely:

wire fraud, that is, to knowingly and with intent to defraud, devise, and intend to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, knowing that they were false and fraudulent when made, and transmitting and causing certain wire communications to be transmitted in interstate commerce, for the purpose of executing the scheme and artifice, in violation of Title 18, United States Code, Sections 1343 and 2.

All in violation of Title 18, United States Code, Section 1349.

COUNT FIVE
Aggravated Identity Theft
[18 U.S.C. § 1028A]

40. On or about March 25, 2012, in the Western District of Texas, and elsewhere, the Defendant,

CHIMENE HAMILTON ONYERI, a/k/a, “Chimu,” a/k/a, “Chimno,”

did knowingly use, without lawful authority, a means of identification of another person, to wit, a Visa credit card number of Victim #2, ending in 6453, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c)(5), namely Conspiracy to Commit Wire Fraud, as charged in Count Four of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT SIX
Aggravated Identity Theft
[18 U.S.C. § 1028A]

41. On or about March 25, 2012, in the Western District of Texas, and elsewhere, the Defendant,

CHIMENE HAMILTON ONYERI, a/k/a, "Chimu," a/k/a, "Chimno,"

did knowingly transfer, possess and use, without lawful authority, a means of identification of another person, to wit, a MasterCard credit card number of Victim #3, ending in 3955, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c)(5), namely Conspiracy to Commit Wire Fraud, as charged in Count Four of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT SEVEN
Aggravated Identity Theft
[18 U.S.C. § 1028A]

42. On or about March 25, 2012, in the Western District of Texas, and elsewhere, the Defendant,

CHIMENE HAMILTON ONYERI, a/k/a, "Chimu," a/k/a, "Chimno,"

did knowingly transfer, possess and use, without lawful authority, a means of identification of another person, to wit, a Visa credit card number of Victim #4, ending in 7954, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c)(5), namely Conspiracy to Commit Wire Fraud, as charged in Count Four of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT EIGHT
Aggravated Identity Theft
[18 U.S.C. § 1028A]

43. On or about March 25, 2012, in the Western District of Texas, and elsewhere, the Defendant,

CHIMENE HAMILTON ONYERI, a/k/a, "Chimu," a/k/a, "Chimno,"

did knowingly transfer, possess and use, without lawful authority, a means of identification of another person, to wit, a MasterCard credit card number of Victim #5, ending in 4795, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c)(5), namely Conspiracy to Commit Wire Fraud, as charged in Count Four of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT NINE
Aggravated Identity Theft
[18 U.S.C. § 1028A]

44. On or about March 25, 2012, in the Western District of Texas, and elsewhere, the Defendant,

CHIMENE HAMILTON ONYERI, a/k/a, "Chimu," a/k/a, "Chimno,"

did knowingly transfer, possess and use, without lawful authority, a means of identification of another person, to wit, a Visa credit card number of Victim #6, ending in 6247, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c)(5), namely Conspiracy to Commit Wire Fraud, as charged in Count Four of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

COUNT TEN
Conspiracy to Commit Wire Fraud
[18 U.S.C. § 1349]

Background

45. “Debit Card Skimming” is a fraudulent scheme in which perpetrators utilize mechanical devices to capture debit card numbers from unsuspecting victims. This is accomplished by using a device known as a “skimmer”, which is placed over the bezel of Automatic Teller Machines (ATMs). The skimmer captures debit card/bank account information from victims’ ATM cards. Perpetrators also attach a camera to the ATM in order to capture victims’ personal identification numbers (PINs). Perpetrators download the debit card/bank account information from the skimmer and encode it onto another card. This card, when combined with the stolen PIN, allows perpetrators to access the bank account of victims who used the altered ATM machine. Perpetrators “cash out,” or convert the stolen information into cash proceeds, by withdrawing funds directly from victims’ bank accounts, purchasing pre-paid gift cards, sending wires or money orders to co-conspirators, among other things. Sometimes the stolen information is used to purchase goods that are later returned for cash or sold. Perpetrators use this kind of “layering” to avoid detection by law enforcement.

The Scheme

46. ONYERI and others, known and unknown to the Grand Jury, participated in a debit card skimming scheme from at least in or about November 2013 to in or about November 2015. ONYERI, MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT, as well as other co-conspirators known and unknown to the Grand Jury, participated in a scheme to

place devices and cameras on ATMs in the Houston, Texas area as well as in other locations in the states of Texas and Louisiana in order to steal victims' bank account/ATM card information and PINs. The process of capturing ATM card/bank account information from ATMs is known as "skimming," and the device used is placed over the bezel, where victims insert their cards so that the device or "skimmer" can read and capture the data on the victims' ATM card. ONYERI and co-conspirators known and unknown to the Grand Jury first began, in or about November of 2013, placing skimming devices on Capital One Bank ATMs because the skimming device that ONYERI constructed, assembled and used fit the bezel of the ATM manufacturer used by Capital One Bank. ONYERI paid co-conspirators to use their homes to store, build and charge the skimming devices. ONYERI paid other co-conspirators to borrow their vehicles or to drive him or to act as lookouts when ONYERI placed the skimming devices onto ATM machines. After Capital One Bank changed all of its ATM machines, ONYERI began attaching skimming devices onto Amegy Bank ATMs. ONYERI also placed skimming devices onto ATMs in Louisiana. ONYERI also placed a camera, most often in an iPod, above the keypad of the ATM on which the skimmers were placed in order to capture victims' PINs. After successfully capturing ATM card/bank account information and PINs, ONYERI, MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT, as well as other co-conspirators known and unknown to the Grand Jury went about the process of "cashing out" the stolen information. "Cashing out" is the process by which the stolen data is converted into cash proceeds. ONYERI used a device to encode the stolen ATM card/bank account information onto blank cards which could then be used, along with the stolen PIN, to purchase items, gift cards, money orders or to withdraw cash.

ONYERI and co-conspirators known and unknown to the Grand Jury used methods to disguise themselves and the vehicles they used throughout the skimming and cashing out processes, such as placing a shirt or sleeve over their faces and placing stolen or paper license plates over the license plates of vehicles. During the cashing out process, ONYERI also paid and utilized co-conspirators, known and unknown to the Grand Jury, who wore burkas to disguise their appearance. The cashing out process often took place at Walmart, where gift cards or money orders were purchased. ONYERI and co-conspirators often traveled to numerous Walmarts in order to spread the cashing out process out and avoid suspicion. During the course of the scheme, ONYERI and co-conspirators, known and unknown to the Grand Jury, cashed out in locations in Texas and Louisiana.

Manner and Means

The scheme consisted of, and was carried out using, the following means and overt acts, among others:

47. In or about November of 2013, ONYERI received the assistance of a co-conspirator who traveled to the United States from outside the United States in order to teach ONYERI how to use skimming devices to acquire ATM card numbers/bank account information and PINs from unsuspecting victims in the United States.
48. From in or about November 2013 to November of 2015, ONYERI and co-conspirators, known and unknown to the Grand Jury, placed skimming devices and cameras on ATM machines in both Texas and Louisiana. ONYERI, with the assistance of co-conspirators, known and unknown to the Grand Jury, successfully placed skimming devices on at least two banks insured by the Federal Deposit Insurance Corporation (FDIC), Capital One Bank

and Amegy Bank. ONYER and his co-conspirators attempted to place skimming devices on other federally insured banks as well.

49. On or about October 17, 2015, ONYERI, with the assistance of co-conspirators, known and unknown to the Grand Jury, placed a skimming device on an Amegy Bank ATM located in Houston, Texas.
50. ONYERI, with the assistance of co-conspirators, known and unknown to the Grand Jury, purchased money orders on the following dates, in the following amounts, using one or the other of the two stolen, skimmed debit card numbers described in paragraph 49 above:

10/24/15	10/25/15	10/26/15	11/2/15	11/3/15
\$1000.00	\$1000.00	\$1000.00	\$1000.00	\$1000.00
\$1000.00	\$1000.00	\$1000.00	\$1000.00	\$1000.00
\$500.00	\$500.00	\$500.00	\$500.00	\$600.00

51. MARCELLUS ANTOINE BURGIN negotiated ten (10) of these money orders and RASUL KAREEM SCOTT negotiated five (5) of them.
52. On or about November 5, 2015, ONYERI, MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT all travelled from Louisiana to Houston and then to Austin, Texas, within the Western District of Texas in a vehicle rented in Houston, Texas, on or about November 3, 2015.
53. On or about November 5, 2015, ONYERI purchased gloves at an Auto Zone, in the Western District of Texas, using a gift card purchased with one of the stolen debit card numbers stolen

and skimmed from the Amegy Bank in Houston, Texas on or about October 17, 2015.

54. On or about November 5, 2015, ONYERI, MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT checked into a motel room, at a Motel 6, located in the Western District of Texas, using a gift card purchased with one the debit card numbers stolen and skimmed from the Amegy Bank in Houston, Texas, on or about October 17, 2015. RASUL KAREEM SCOTT presented the gift card at the front desk of the motel in order to pay for the room.
55. On or about November 6, 2015, in the Western District of Texas, MARCELLUS ANTOINE BURGIN and RASUL KAREEM SCOTT purchased clothing at Walmart using a gift card purchased with one of the debit card numbers stolen and skimmed from the Amegy Bank in Houston, Texas on or about October 17, 2015.

The Charge

56. Paragraphs 45 through 55 of this Indictment are re-alleged and incorporated by reference as though fully set forth herein.
57. From at least in or about November 2013 to in or about November 2015, the exact dates being unknown, in the Western District of Texas and elsewhere, the Defendants,

**CHIMENE HAMILTON ONYERI,
a/k/a, "Chimu," a/k/a, "Chimno,"
MARCELLUS ANTOINE BURGIN,
a/k/a, "Southwest,"
a/k/a, "Chi,"
a/k/a, "Chi-town," and
RASUL KAREEM SCOTT,
a/k/a, "N.O.,"**

did knowingly and willfully conspire and agree with others known and unknown to the Grand

Jury, to commit certain offenses against the United States, namely:

wire fraud, that is, to knowingly and with intent to defraud, devise, and intend to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, knowing that they were false and fraudulent when made, and transmitting and causing certain wire communications to be transmitted in interstate and foreign commerce, for the purpose of executing the scheme and artifice, in violation of Title 18, United States Code, Sections 1343 and 2.

All in violation of Title 18, United States Code, Section 1349.

COUNT ELEVEN
Aggravated Identity Theft
[18 U.S.C. § 1028A]

58. On or about November 5, 2015, in the Western District of Texas, and elsewhere, the Defendants,

CHIMENE HAMILTON ONYERI,
a/k/a, "Chimu," a/k/a, "Chimno,"
MARCELLUS ANTOINE BURGIN,
a/k/a, "Southwest,"
a/k/a, "Chi,"
a/k/a, "Chi-town," and
RASUL KAREEM SCOTT,
a/k/a, "N.O.,"

did knowingly transfer, possess and use, without lawful authority, a means of identification of another person, to wit, a debit card number of Victim #7, ending in 2627, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c)(5), namely Conspiracy to Commit Wire Fraud, as charged in Count Nine of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

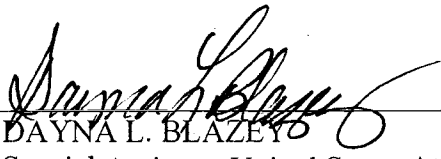
A TRUE BILL ✓
**ORIGINAL SIGNATURE
REDACTED PURSUANT TO
E-GOVERNMENT ACT OF 2002**
✓ FOREPERSON

RICHARD L. DURBIN, JR.
United States Attorney

By: _____


GREGG N. SOFER
Assistant United States Attorney

By: _____


DAYNA L. BLAZEY
Special Assistant United States Attorney